



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/628,692	07/28/2000	W. Olin Sibert	7451.0025-00	3388

22852 7590 11/28/2005

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER

COLIN, CARL G

ART UNIT PAPER NUMBER

2136

DATE MAILED: 11/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/628,692	Applicant(s) SIBERT, W. OLIN	
	Examiner Carl Colin	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 June 2005.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 7-13 and 28-47 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 7-13 and 28-47 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07/28/2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/16/2005 has been entered.

Response to Arguments

1.1 In response to communications filed on 6/16/2005, applicant cancels claims 1-6 and 14-27; amends claims 7 and 9 and adds claims 28-47. The following claims 7-13 and 28-47 are presented for examination.

1.2 Applicant's arguments, pages 9-12, filed on 6/16/2005, with respect to the rejection of claims 1-26 have been fully considered, but they are not persuasive as amended. Applicant has amended claim 7 to recite "checking the response against the credential and determines whether the predetermined portion of the application has been modified", which raises new matter as discussed below. Benson discloses checking the response against a key file to determine whether the program is valid or has been tampered with (see column 12, line 50 through column 13, line 18 see also column 1, lines 48-62 and column 2, line 48-51). Shavit further discloses the amended limitation as recited in amended claim 7. In addition, this feature and the

Art Unit: 2136

computing step as disclosed in claims 1 and 14 can also be found in the (*Applicant IDS*) US Patent 5,745,678 to Herzberg (see claims in Herzberg). Herzberg further discloses that the random selection of data portions of the electronic item provides the benefit of reducing forgery (*column 6*). Applicant adds new claims that recite similar limitations to claim 7 and they are also disclosed by the cited art for the last Office Action. Applicant now relies on a trusted element to overcome Benson, Shavit, and Herzberg. The use of a validation module residing in a protected environment (protected space in the hard disk, tamper resistant space, smart card , dongle, etc.) to protect the execution of a program in a user computer is very well known in the art and Benson suggests using protecting environment or secure space for defense against attacks in column 16 as discussed below. Benson also suggests integrating the functions of the server and the computer user (that executes the program) in the same machine by having the program reside in one address space and the server in a different address space (column 16, lines 47-59 and column 14, lines 5-26). Using the second program and license server program of Shavit in a protected environment in the same machine as the first program would have also been obvious to one skilled in the art as suggested by Benson. Applicant has not overcome the rejection by amending the claims, therefore the claims remain rejected under the same references as in the last Office Action.

Specification

2. The disclosure is objected to because of the following informalities: the description of element 108 is not consistent with the drawing. For instance, on pages 30-31, element 108 is

Art Unit: 2136

being referred to protected processing environment, trusted element, and secure execution space.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3.1 Claim 7 and the intervening claims are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant's disclosure fails to recite issuing a challenge requesting a response from the insecure arrangement. The specification, on the other hand, page 31, lines 13-22, recites challenging application 600 or other agent. Application 600 is merely used "at least in part within insecure environment". The specification fails to describe checking the response against the credential and determines whether the predetermined portion of the application has been modified. On the other hand, page 31, lines 13-22, recites comparing the responses to deny service to application 600 or take other appropriate action if the comparison fails.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4.1 **Claims 7-13 and 28-47** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,047,242 to **Benson** in view of US Patent 6,009,543 to **Shavit**.

4.2 **As per claims 7, 8, 32, 39, and 45, Benson** substantially discloses a trusted element for use with a computer system including an insecure arrangement for using an application, the trusted element comprising: in one embodiment, **Benson** discloses a server that meets the recitation of trusted element, that may be on a separate address space and the program is executing in a different space on the user machine considered as insecure, both the server and the program are in the same machine (column 16, lines 55-59 and column 14, lines 5-26), in another embodiment, the program may reside on a floppy disk or CD ROM or downloaded from the Internet (see column 16, lines 8-12). **Benson** discloses a trusted element comprises a decryptor that decrypts a credential (key file) associated with the application, for example (see column 12,

Art Unit: 2136

lines 63-65); a validator that validates at least one digital signature corresponding to the credential, for example (see column 12, line 55 through column 13, line 15); **Benson** discloses a challenge/response means that meets the recitation of a challenge generator that selects, based at least in part on the credential, at least one predetermined portion of the application, and issues a challenge requesting a response from the insecure arrangement, the response providing a computation of at least one value based on the selected predetermined portion of the application, for example (see column 12, line 55 through column 13, line 52 and column 10, line 47 through column 11, line 38), **Benson** discloses that the key file contains hidden information concerning selective activation of services of the protected program such as execution of a Print service, Save-On-Disk service, date a particular service may execute, etc. that meets the recitation of “predetermined portion of the application including some codes” and further discloses performing a validation (authentication) on the key file (credential) to determine whether the key file is valid or has been tampered or whether to deny service to the program that meets the recitation of determining whether the predetermined portion of the application has been modified (see column 17, lines 1-25 and column 10, lines 29-42; column 12, lines 11-15); **Benson** discloses the challenge/response in another embodiment, for example (see column 9, lines 25-45; column 17, line 25 through column 18, line 55; and column 19, lines 15-53); and a response checker that checks the response against the credential and determining whether the predetermined portion of the application has been modified, for example (see column 12, line 50 through column 13, line 18 see also column 1, lines 48-62 and column 2, line 48-51). **Benson** does not explicitly teach randomly selecting one of the one of the predetermined plural portions from plural predetermined portions. However, **Shavit** in an analogous art teaches randomly

Art Unit: 2136

selecting a predetermined portion of the application, the predetermined portion of the application including some codes, for example (see column 11 lines 49-57 and column 14, lines 39-63, and column 15, lines 55 et seq.) and determining whether the predetermined portion of the application has been modified (column 16, lines 30-55); randomly selecting one of the predefined plural portions, for example (see column 11 lines 49-57). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Benson** to select randomly the predetermined portion from plural predetermined portions as taught by **Shavit** in order to maintain control over those parties able to use the software, for example (see column 12, lines 56-58). One skilled in the art would have been motivated to do so because by randomly selected portion needed for the user program to function, it would render it relatively difficult to replace the functionality provided in the missing portion without input from the other program in the trusted side (see column 12, lines 30-58), thereby maintaining control over those parties able to use the software as suggested by **Shavit**.

As per claims 10-11, the combination of **Benson** and **Shavit** discloses the limitation of wherein the challenge generator requests the application to compute a cryptographic hash of the selected portion (see **Benson**, column 13), see also **Shavit**, column 16, lines 30-60.

As per claims 28, 35, and 42, claims 28 and 35 recite similar limitations as claims 7 and 11, except for using random selection of the credential and denying access to services when the program is not validated. **Benson** discloses denying access to services when the program is not authenticated and **Shavit** further discloses challenge based on random selection requesting the

Art Unit: 2136

application to provide hash of portion of the application as discussed in claims 7, 8 and 11 above.

Claim 42 recites an appliance comprising a secure execution space, an insecure execution space a trusted element operable to execute within the secure execution space. **Benson** discloses a server that meets the recitation of trusted element, and suggests that the server program may be on a separate address space and the program is executing in a different space on the user machine considered as insecure, both the server and the program reside in the same machine (column 16, lines 55-59), in another embodiment, the program may reside on a floppy disk or CD-ROM or downloaded from the Internet (see column 16, lines 8-12). Therefore, claims 28, 35, and 42 are rejected on the same rationale as the rejection of claims 7, 8, and 11.

As per claim 43, Benson also suggests using smart card and dongle that meets the recitation of protected environment. It would have been obvious to one skilled in the art to implement the license server in a smart card or dongle in order to protect the challenge mechanism of the license server as suggested by **Benson** (column 16, lines 13-17, lines 40-46). It is also very well known in the art that a program operating in a user computer when protected by a validation system is protected with an authentication program or cryptographic processors that reside in a protected environment. It would also have been obvious to one ordinary skill in the art to use a smart card or any other protecting environment as known in the art to protect the second program and the server program of Shavit for protection against attacks as suggested in **Benson**.

As per claims 9, 12, 34, 41, and 47, the combination of **Benson** and **Shavit** discloses the claimed system of claim 7. **Shavit** further teaches the limitation of: wherein the challenge generator issues the challenge during execution of the application by the insecure computing arrangement (see column 12, line 53 through column 13, line 4); and wherein the challenge generator selects a virtual path within the application (see column 5, lines 55-67). Therefore, these claims are rejected on the same rationale as the rejection of claims 7 and 8 above.

As per claim 13, the combination of **Benson** and **Shavit** discloses the limitation of wherein the challenge generator selects a byte range within the application (see **Benson**, column 9, lines 40-63).

As per claims 30, 31, 37, 38, and 44, **Benson** discloses the limitation of further including the step of digitally signing the credential and at least in part encrypted (see column 11, lines 22-51).

As per claims 29, 33, 36, 40, and 46, the combination of **Benson** and **Shavit** discloses repeating the challenges and portions of the application may overlap (see **Shavit**, column 15, line 55 through column 16, line 55). Therefore, these claims are rejected on the same rationale as the rejection of claims 7 and 8 above.

Art Unit: 2136

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin

Patent Examiner

November 21, 2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100